Privacy Impact Assessment

For

EDUCATE

Date
October 28, 2009

Point of Contact:

System Owner: Lisa Mendis

Author: Michael Rohde

Office of the Chief Information Officer

U.S. Department of Education

1. What information will be collected for the system (Ex. Name, Social Security Number, annual income, etc)?

EDUCATE is the infrastructure that supports primary IT services for the Department of Education and is considered a General Support System. EDUCATE serves as the chief communications link between Headquarters' offices and the various regional and satellite offices.

EDUCATE primarily consists of circuits, routers, switches, servers, and wireless messaging services, along with printers, workstations, and in many cases, telephones that provide real-time communication within the entire department. EDUCATE serves the Department with critical information resources and reaches out to customers via the following:

EDCIS - The EDUCATE Data Center Information System is the infrastructure that supports primary IT applications for ED and is considered a GSS. EDCIS primarily consists of servers providing the following:

- Local Area Network (LAN) Services – interconnecting employees with application, web, database, file and print services within an office building.

Development Services – update and maintain the agency's Internet presence (ED.gov website), the employee intranet (connectED) and developing custom business applications

EDNIS - The EDUCATE Network Infrastructure System is the infrastructure that serves as the network backbone for EDUCATE and its supported systems and applications.

EDNIS EDUCATE primarily consists of circuits, routers, and switches that provide real-time communication within the entire department. EDUCATE serves ED with critical information resources and reaches out to ED customers via the following:

- Wide Area Network (WAN) Services – interconnecting employees to the Internet, web-based services, and the LANs throughout the EDUCATE network.
- Metropolitan Area Network (MAN) Services – interconnecting multiple LAN locations in the Washington, DC area.
- Local Area Network (LAN) Services – interconnecting employees with application, web, database, file and print services within an office building.
- IP Communications Services – provide employees with a suite of communications services, including IP-based voice (VoIP), unified messaging, conferencing and automated call distribution.

EDMASS - The EDUCATE Mass Storage System (EDMASS) is the General Support System that supports primary data storage functionality for the Department of Education. The EDMASS environment utilizes Network-attached Storage (NAS) and also includes about 1TB of SAN in a multi-protocol, segmented environment, involving two locales. Large NAS heads are located at the PTC site and the FTC site. These NAS heads are essentially self-contained computers connected to a network, with the sole purpose of

supplying file-based data storage services to other devices on the network. The operating system and other software on the NAS units provide the functionality of data storage, file systems, and access to files, and the management of these functionalities. The units are not designed to carry out general-purpose computing tasks, although it may technically be possible to run other software on them.

PEDS - The Department of Education PEDS provides reliable wireless device email redirection, cellular phone service, and internet access for approximately 950 users.

The PEDS consists of the following sub-components:

- Blackberry Enterprise Server
- Goodlink Mobile Messaging System
- Microsoft SQL Database for Blackberry Server

The Blackberry Enterprise Server (BES) provides wireless access to email. The BES integrates with the Department of Education Microsoft Exchange email system to automatically deliver email to the PED.

Goodlink Mobile Messaging System is a wireless device email redirection platform similar to Blackberry Enterprise Server. There are two wireless devices supported by Goodlink. They are Nokia E62's which are used to provide assistive technology (convert on-screen text to speech) to visually impaired users. All other users utilize the blackberry portable electronic device.

Cellular phone service is provided by Verizon and AT&T. Internet access is provided through the cellular carrier's data network and both phone and internet access from the PED's is independent of and outside of the PED accreditation boundary.

The PEDS components include Blackberry Enterprise Server 4.1 running on Microsoft Windows Server 2003 R2 SP2. Goodlink is Good Mobile Messaging 5.0 running on Microsoft Windows Server 2003 R2 SP2. The SQL database is for database replication for the PEDS disaster recovery.

EMAIL - The Department of Education Email System provides a reliable messaging system, with built-in protection against spam and viruses.

The Email System consists of the following sub-components:

- Microsoft Exchange 2007
- Symantec AntiVirus Messaging Component
- Postini Email Security Service

The Email Systems utilize Microsoft Exchange 2007 running on Microsoft Windows Server 2003 R2 Service Pack (SP)2, and Microsoft Outlook 2007 serves the client end users at their desktop workstation and Outlook Web Access (OWA) provides users remote Web-based

messaging connectivity. Users throughout the organization can access e-mail, voice mail, calendars, and contacts from a wide variety of devices and from any location.

The Email Archiving and Records Management System provides a central archiving system for email messages, and calendar entries and a search mechanism (e-Discovery) for retrieving data from the archive.

The Email Archiving and Records Management System consists of the following sub-components:

- EMC EmailXtender
- EMC DiskXtender

The Email Archiving and Records Management Systems utilize Microsoft Windows 2003 R2, SP 2 and EMC's EmailXtender, DiskXtender, and LicenseServer. In addition Microsoft SQL Enterprise Edition SP2 is the database application.

Service Desk - The Service Desk System consists of two applications, the Operational Process Application Suite (OPAS) system and the EDUCATE Self Help Portal (ESHP). The OPAS system is the Perot Systems standard for tracking and reporting records related to Service Management processes (incident management, change management, request management, problem management and configuration management). OPAS is built on the Remedy® Action Request System. The OPAS system provides ED employees and customers with Service Management support through the non-public Local Area Network (LAN) provided by EDUCATE's Network Infrastructure system.

Actions performed within OPAS include:

- Creating new records
- Searching records
- Modifying records
- Reporting information to screen, file or printer
- Creating macros and saving searches to ease workflow operations

The EDUCATE Self Help Portal (ESHP) is a content management system which enables authenticated users on the ED.GOV domain to see current information about outages, create service desk tickets, and view the status of their existing tickets. The system uses Integrated Windows Authentication (aka, NTLM) to identify users visiting the site without requiring them to log in again.

SOC -The EDSOC manages all of the Department of Education (DoED) Intrusion detection systems (IDS), Intrusion Prevention Systems (IPS), anti-virus (AV) services, Security Information Management (SIM) systems, Content Filtering, managed authentication systems (TACACS), and reporting. In addition the EDSOC provides around the clock (24x7) staffing

responsible for maintaining situational awareness of the ED information technology infrastructure including the EDUCATE Data Center Information System (EDCIS). EDSOC primarily consists of the following systems/services:

- Coverage of the ED Security Operations Group Phone Line
- Monitoring of the ED Security Operations Team group distribution list
- Security Information Management/Security Event Management
- Anti-Virus monitoring, alerting, investigation, and management
- Host and Network based Intrusion Detection Systems (HIDS/NIDS)
- Host and Network based Intrusion Prevention Systems (HIPS/NIPS)
- Incident Investigation and Response
- Managed Authentication Systems (TACACS)
- Content Filtering of internet access
- Daily Reporting

The EDSOC supports the entire ED information technology infrastructure and over 5,200 users in Washington, DC and multiple locations across the United States.

Desktop - The Desktop system contains the workstations that allow Department of Education employees to conduct daily tasks to fulfill the Department's mission using a variety of Office Suites, Commercial off the Shelf (COTS) software applications, custom applications, system tools, and applications that directly support the functions of the Department. The Department is migrating the majority of the Desktops to a Windows Vista image to improve security and performance of the systems. These migration efforts have been taking place since July 2008 and plan to be completed during the summer of 2009.

EDUCATE is the principal IT infrastructure component for the Department and does not directly collect privacy data. Privacy data is collected by some of the 140-plus systems that are hosted by the network. These systems include applications for the Office of the Chief Financial Officer, Office for Civil Rights, Office of Communications and Outreach, Office of Elementary and Secondary Education, Office of Inspector General, Office of Management, Office of Postsecondary Education, Office of the Secretary, Office of Special Education and Rehabilitative Services. Some of the applications residing on the network that collect privacy date include, but are not limited to, the following:

- Education Central Automated Processing System (EDCAPS)
- EDSTAR
- Case Services Reporting System
- FOIAXpress
- Grants Administration and Payment System (GAPS)
- Jacob K. Javitz Fellowship System
- Migrant Student Immigration Exchange (MSIX)
- Data Analytic System (ODAS)
- Secretary's Communications Control System
- Case and Activity Management System (CAMS)
- Presidential Scholars Program

- Travel Manager System
- TRIO Programs Annual Performance Report System

These applications collect various privacy data including, but not limited to, names, addresses, telephone numbers, social security numbers, email addresses, and bank account numbers for students and other individuals applying for and receiving loans and grants. The major applications maintain and control data collected for the use of the offices.

2. Why is this information being collected?

EDUCATE does not collect privacy data, however many applications that reside on the network do collect privacy data. EDUCATE hosts many of the Department's systems pertaining to student loans, grant information, and educational services. The offices identified in Question One maintain and control the type of data collected for each system. The PIAs addressing these systems can be found at the Department's website at: http://www.ed.gov/notices/pia/index.html.

3. How will the information be used?

Some of the applications residing on the EDUCATE network collect privacy data for specific uses by the applicable Principal Office in carrying out its mission as specified in the PIA at the Department's website at: http://www.ed.gov/notices/pia/index.html.

4. Will this information be shared with any other agency or entity? If so, with whom?

 Under specific circumstances, it may be necessary to disclose privacy data. As a host facility EDUCATE does not collect or disseminate data however, EDUCATE may be tasked to send files/tapes to other agencies on behalf of the offices listed in Question One. Please refer to each system's PIA at: http://www.ed.gov/notices/pia/index.html, for information about that specific system's disclosures.

5. Describe the notice or opportunities for consent that are provided to individuals about what information is collected and how that information is shared with other organizations. (e.g., posted Privacy Notice).

EDUCATE hosts many of the Department's systems that administer student loans, grants, and education services. The Principal Offices listed in Question One maintain and control the type of data collected for each system, and they provide any relevant notice or opportunities for consent. The PIAs addressing these systems can be found at the Department's website at: http://www.ed.gov/notices/pia/index.html. The Department privacy notice is located at the following link: http://www.ed.gov/notices/privacy/index.html.

6. How will the information be secured?

EDUCATE has been secured at the physical security, operating system, database, and network infrastructure levels. The network complies with the security controls and procedures described in the Federal Information Security Management Act (FISMA), National Institute of Standards

and Technology (NIST) Special Publications, and Federal Information Processing Standards (FIPS). The EDUCATE network has been certified and accredited, and received an Authority to Operate on August 1, 2008. Please refer to the EDUCATE System Security Plan for the specific Management, Operational, and Technical security controls deployed on the system. The System Security Plan details how the following security control families are implemented on the system:

- Risk assessment
- Planning
- System and services acquisition
- Certification, accreditation, and security assessments
- Personnel security
- Physical and environmental security
- Contingency planning
- Configuration management
- Maintenance
- System and information integrity
- Media protection
- Incident response
- Awareness and training
- Identification and authentication
- Access control
- Audit and accountability
- System and communications protection.

Some specific security controls in place include:

• Operating systems and infrastructure devices are hardened in accordance with NIST and Department guidance.

• Intrusion Detection Systems are deployed at the Intranet and Internet edges and are actively monitored by the Security Operations Center (SOC).

• Vulnerability scans are conducted periodically to ensure supporting systems and all applications are at the highest state of security and are patched accordingly

7. Is a system of records being created or updated with the collection of this information?

No. A Privacy Act System of Records is not being created or updated because the EDUCATE network serves only as a host for systems that contain privacy data. Please refer to each individual system's PIA for information regarding whether that system is a Privacy Act System of Records, and as such, has published a System of Records Notice in the Federal Register.

8. List the web addresses (known or planned) that will have a Privacy Notice.

Please refer to each individual system's PIA for the specific web addresses that contain a Privacy Notice. Also, the Department privacy notice is located at the following link:

http://www.ed.gov/notices/privacy/index.html.